(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

[Continued on next page]

(54) **Title:** FRAUD DETECTION METHOD FOR MOBILE TELECOMMUNICATION NETWORKS

```
AuthenticationFailureReport ::= OPERATION          --Timer m
    ARGUMENT
        authenticationFailureReportArg    AuthenticationFailureReportArg
    RESULT
        authenticationFailureReportRes    AuthenticationFailureReportRes
    -- optional
    ERRORS {
        SystemFailure, {
        UnexpectedDataValue,
        UnknownSubscriber }
```

```
AuthenticationFailureReportArg ::= SEQUENCE {
    imsi                IMSI,
    failureCause        FailureCause,
    accessType          AccessType,
    re-attempt          BOOLEAN,
    vlr-Number          [0]   ISDN-AddressString    OPTIONAL,
    sgsn-Number         [1]   ISDN-AddressString    OPTIONAL,
    extensionContainer        ExtensionContainer    OPTIONAL,
    ... }
```

```
AccessType ::= ENUMERATED {
    call                (0)
    emergencyCall       (1)
    locationUpdating    (2)
    supplementaryService (3)
    shortMessage        (4) }
```

(57) Abstract: The present invention provides a fraud detection method for third generation mobile telecommunication systems using data related with unsuccessful authentication procedures, such us access type, authentication re-attempt and server address as secondary fraud indicators. Said date are included in predefined-type fields of the authentication failure report message sent form the Serving Environment back to the Home Environment in said authentication procedures, stored in the Home Location Register and forwarded to the Fraud Detection Systems for processing in conjunction with primary fraud indicators, for fraud detection purposes.

WO 02/43424 A1

FRAUD DETECTION METHOD FOR MOBILE TELECOMMUNICATION NETWORKS

Field of the Invention

This invention relates generally to the fraud
5   detection in mobile telecommunication networks. More specifically, this invention relates to a method for obtaining, storing and processing significant data for fraud detection.

Background

10   The security group in the 3rd Generation Partnership Project, in charge of Security Architecture (hereinafter referred to to as "3GPP (SA3)"), have introduced in the Technical Specification Group Services and System Aspects 33.102 v3.5.0 (hereinafter referred to as 3G TS 33.102) a
15   new procedure called Authentication Failure Report. Besides, the standard signalling messages and message parameters involved in said new procedure are described in the Mobile Application Part (hereinafter referred to as MAP) specification 29.002 v3.4.0 issued by the 3GPP
20   Technical Specification Group Core Network (hereinafter said specification is referred to as 3GPP TS 29.002).

Most of the previous generations of mobile systems already make use to some extent of Authentication procedures to ensure that a user accessing the mobile
25   network is the one who claims. And not only the mobile users but rather the different network entities involved in certain mobile communications are already objects of authentication to some extent. Any interested reader can refer to Technical Specification 03.20 for GSM "Security
30   related network functions" from the European Telecommunication Standard Institute (generally known and

- 2 -

hereinafter referred to as TS ETSI GSM 03.20, "Security related network functions"). These authentication mechanisms are intended to preclude the access to the mobile networks and mobile services for unauthorised users

5 or network entities. Moreover, the needs for authentication of mobile users and network entities do not only make sense for the Pan-European mobile networks like GSM, but also for the Pan-American mobile networks like those based on the Interim Specification number 41 (hereinafter referred to as

10 IS-41), for example.

These authentication mechanisms from previous generations of mobile systems are naturally evolving, including new security features, within the scope of the 3rd mobile systems generation (hereinafter simply referred to

15 as 3G). Nowadays, a well-known instance of 3G is the Universal Mobile Telecommunication System (hereinafter referred to as UMTS) and security aspects, security features and security architecture, such as those related to subscriber Authentication and network entity

20 Authentication, are described in the technical specification above mentioned, 3G TS 33.102.

Irrespective of particular network architectures that these mobile systems generations might have, including different standards such as the Pan-European or Pan-

25 American standards above mentioned, some commonalties are pointed out following this to better understand the wider scope of the present invention.

On the one hand, any mobile network like the one in Fig.-1- can be regarded as consisting of a Home Environment

30 (N-1000) (hereinafter referred to as HE), a Serving Network (N-2000) (hereinafter referred to as SN), and a number of

- 3 -

mobile terminals, namely User Equipment (N-3000) (hereinafter abbreviated as UE). On the other hand, such a mobile network in Fig.-1- can be regarded as consisting of a Core Network (N-0100) and an Access Network (N-2200)
5   wherein the former consists of the Home Environment plus the Serving Network excluding network entities from the Access Network.

Furthermore, the existing mobile systems already offer support with shared and dedicated network infrastructure
10 for both Circuit Switched (N-2120) (hereinafter CS) services, such as pure telephony, as well as Packet Switched (N-2110) (hereinafter PS) services, such as other data transmission oriented services. The packet switched services have been lately introduced over the 2G mobile
15 systems. A well-known instance of the existing technology to support the packet switched services is the GSM Packet Radio System (hereinafter abbreviated as GPRS).

The HE (N-1000) represents all the network entities which uniquely handle and give support to home subscribers
20 of a certain Public Land Mobile Network (hereinafter PLMN). For example, the Home Location Register (N-1102) (hereinafter HLR) is the network entity of a certain PLMN in charge of holding all the subscription data for home subscribers of said PLMN, and thus part of the HE. Another
25 network entity also part of the HE is the Authentication Centre (N-1101) (hereinafter AUC), which is in charge of generating and providing authentication and key data either as triplets for GSM or as vectors for UMTS. These authentication and key data are respectively intended to
30 check that any home subscriber is the one who claims, wherever he or she is accessing the mobile network, and to

- 4 -

provide the means for ciphering the transmission through the radio path. A more detailed explanation of usage and procedures for 2G and 3G Authentication is further introduced in this description.

5   The SN (N-2000) represents all the network entities or resources in a certain PLMN that give service to mobile subscribers roaming in such a PLMN irrespective of being home or visitor subscribers. For example, the Mobile Service Switching Centre (also called Mobile Switching

10   Centre, and hereinafter abbreviated as MSC) constitutes the interface between the radio system and the fixed networks. Said MSC is the network entity in charge of all switching functions related to Circuit Switching (CS), controlling the location and routing area wherein a certain subscriber

15   is roaming, and thus part of the SN. Another network entity part of the SN is the Visitor Location Register (hereinafter abbreviated as VLR). Said VLR is a subscriber database holding relevant subscription data from all the subscribers currently roaming in the area controlled by

20   such a VLR, and which were obtained from the corresponding HLR where each subscriber has his or her own subscription. At present, most of the existing GSM or IS-41 based mobile systems have implemented both entities collocated so that they are usually referred to as a unique entity (N-2121) by

25   the abbreviation MSC/VLR. Furthermore, the evolved version of said MSC/VLR for the 3G mobile systems is generally referred to as 3G MSC/VLR. In a similar manner as said MSC/VLR is in charge of relevant subscription data, and carries out the CS functions, the Serving GPRS Support Node

30   (N-2111) (hereinafter abbreviated as SGSN) performs similar tasks for PS functions and corresponding subscribers. The SGSN holds relevant subscription data from all the

- 5 -

subscribers currently roaming in the area controlled by such an SGSN, and which were obtained from the corresponding HLR where each subscriber has his or her own subscription. Said SGSN is also in charge of all switching functions related to Packet Switching (PS), controlling the location and routing area wherein a certain subscriber is roaming, and thus part of the SN. Furthermore, the evolved version of said SGSN for the 3G mobile systems is generally referred to as 3G SGSN. Besides, Fig.-1- also shows a representative access network node for completeness purpose, namely the UMTS Terrestrial Radio Access Network (N2201) (hereinafter referred to as UTRAN).

The authentication procedure, generally speaking, is initially performed at the first radio contact from a mobile subscriber trying to gain access to the mobile network. In accordance with the specification 3G TS 33.102 above mentioned, the method was chosen in such a way as to achieve maximum compatibility with the current GSM security architecture and facilitate migration from GSM to UMTS. The method is composed of a challenge/response protocol identical to the GSM subscriber authentication and key establishment protocol combined with a sequence number-based one-pass protocol for network authentication. Even though this procedure is basically described following this, an interested reader could get more detailed explanations by reading said specification 3G TS 33.102 version 3.5.0, sections 5.1.1 and 6.3.1.

The challenge/response method from GSM formally starts by a request from the SN VLR/SGSN to the HE HLR/AUC to generate and provide authentication triplets (authentication vectors under 3G). Said authentication

triplet consists of a random number RAND, an expected
response XRES, and a ciphering Key CK. Each authentication
triplet is valid, in principle, for just one authentication
process, though they can be reused under certain
5   circumstances. At reception of said triplets from the HE,
the VLR/SGSN sends to the GSM Subscriber Identity Module
(hereinafter abbreviated as SIM), which is responsible for
performing GSM subscriber authentication and key agreement
at the subscriber side, the received random number RAND. At
10   the subscriber side, the RAND and a pre-stored subscriber
identity key KI are used as inputs to algorithms A3 and A8
to produce a signed response SRES and a ciphering key CK.
The SIM returns the SRES obtained to the challenger
VLR/SGSN, which will check the lately received SRES versus
15   the stored XRES. Provided that they match each other, the
authentication is found to be successful and the CK, that
both VLR/SGSN and SIM have, can be locally used to cipher
further communication through the radio path.

Fig.-2-   schematically   presents   how   this
20   challenge/response authentication method evolves for UMTS
networks. In accordance with 3G TS 33.102, the HE HLR/AUC
is requested (S-200) to generate and provide authentication
vectors consisting of a random number RAND, an expected
user response XRES, a cipher key CK, an integrity key IK,
25   and a network authentication token AUTN. Upon receipt of
such a request from the SN VLR/SGSN, the HE HLR/AUC
generates (B-090) and sends an ordered array of n
Authentication Vectors (S-210) (the equivalent of GSM
"triplets", and hereinafter referred to as AV) to the SN
30   VLR/SGSN wherein these authentication vectors are stored
(B-100). As for GSM, each authentication vector is valid
for one authentication and key agreement process between

- 7 -

the VLR/SGSN and the User Services Identity Module (hereinafter referred to as USIM). As opposite to GSM, these vectors cannot be reused. In a security context, such a USIM is responsible for performing UMTS subscriber and
5   network authentication, and key agreement. Said USIM should also be capable of performing GSM authentication and key agreement to enable the subscriber to roam easily into a GSM Radio Access Network. When the VLR/SGSN initiates an authentication and key agreement, it selects the next
10 authentication vector from the array (B-110) and sends the parameters RAND and AUTN to the user (S-220). The USIM checks whether AUTN can be accepted by computing the anonymity key AK as a function of RAND (B-120) and then, once AK is known, by extracting from the received AUTN the
15 sequence number SQN (B-130), the authentication management field AMF (B-140), and the message authentication code MAC (B-150). Next USIM computes XMAC as a function of RAND, SQN, and AMF (B-160) and compares such an XMAC value with the previously extracted MAC (B-170). Provided that these
20 values are found to be different, the user sends a *"user authentication reject"* (S-230) back to the VLR/SGSN with an indication of the cause, and the procedure is abandoned. This result is understood as an unsuccessful network authentication. In this case, the SN VLR/SGSN shall
25 initiate an Authentication Failure Report (S-240) towards the HE HLR indicating "wrong network signature" as failure cause. On the other hand, when MAC and XMAC match each other, USIM verifies that SQN value is in the correct range (B-180). Provided that USIM considers SQN is not in due
30 range, it sends a *"synchronisation failure"* (S-250) back to the VLR/SGSN including an appropriate parameter, and the procedure is abandoned. If SQN is in range, USIM considers the network as successfully authenticated and computes a

- 8 -

response RES, a cipher key CK and an integrity key IK by applying different functions to different combinations of authentication parameters (B-190). Said response RES is sent back to the VLR/SGSN (S-260). The VLR/SGSN compares

5   the received RES with XRES (B-200). If said RES and XRES match each other the VLR/SGSN considers the authentication and key agreement exchange to be successfully completed. The established keys, CK and IK, will be locally used to cipher further communication through the radio path. But,

10 if XRES and RES are found to be different, the SN VLR/SGSN shall initiate an Authentication Failure Report (S-270) procedure towards the HLR indicating "wrong user response" as failure cause. Moreover, the SN VLR/SGSN may also decide to re-attempt a new identification and authentication

15 procedure towards the user.

In accordance with the 3G TS 33.102, this mechanism somewhat described above achieves mutual authentication by the user and by the network, showing knowledge of a secret key K which is shared between and available only to the

20 USIM and the AUC in the user's HE. Moreover, a network authentication failure detected at the user side, namely by USIM, or a user authentication failure detected at the network side, namely by SN VLR/SGSN, they both trigger the new procedure "Authentication Failure Report".

25   The aim of this new procedure is to inform the Home Environment (HE) when an authentication has failed, including the failures due to an unsuccessful network authentication or unsuccessful user authentication. However, this procedure is not applicable to

30 synchronisation failures, which are reported by a different procedure. In summary, such an Authentication Failure

- 9 -

Report procedure is merely used to report the kind of failure (user or network) and the International Mobile Subscriber Identity (hereinafter referred to as IMSI) towards the HE.

5   At this point, another significant aspect to comment on, background of the present invention, is the fraudulent use of mobile services and mobile networks. One of the highest fraud exposures in mobile networks is due to call selling using supplementary services, and especially due to
10   the difficult control of subscriber activities when said subscribers are roaming in a PLMN other than the home network. In this context, Call Selling is a fraudulent activity that consists in using a mobile subscription to sell long distance calling service throughout the world,
15   below market price, and with the intention of not paying for such calls to the network operator. For example, a mobile subscriber may initiate fraudulent call selling by making use of Call-Forwarding service in HLR and Third-Party call service. Still another example of fraud is the
20   Roaming Fraud. As a matter of fact, international roaming is possible for most of mobile systems wherein the fraud is carried out by initiating call selling operations by using foreigners subscriptions in certain countries where roaming is possible. This fraudulent activity can hardly be
25   detected on time to act because of late reporting and billing from the operators involved. These and many other fraud risks have been identified and justify the efforts to provide the means to prevent fraud, and also to detect the specific fraudulent activity. In this respect, most of the
30   mechanisms introduced around the authentication procedures are more oriented to fraud prevention than to the fraud detection as such.

Nevertheless, and assuming that said fraud prevention is not always achieved, great efforts are made to develop fraud detection systems robust enough to ensure a rapid detection of fraudulent activities. An important aspect to
5 determine is the criteria to unambiguously identify that a fraud is committed. Rather than focusing on legal frames to determine fraud, this description is aimed to outline activities and situations which, isolated or combined, can indicate a fraudulent use of mobile network resources.

10 To this end, a new network entity generally known as Fraud Detection System (hereinafter referred to as FDS) was introduced in mobile networks. Said FDS is responsible for detecting the existence of fraud by analysing a certain amount of indicators. Such indicators are classified
15 attending to type and way of use. As classifying indicators by type, the following three categories can be identified:

i) <u>Usage indicators</u> are defined by some criteria relating to the way in which a mobile telephone is used. Most types of fraud are characterised by unusually high
20 usage. For example in call selling activities, the mobile terminal needs to register several call-forwarding numbers.

ii) <u>Mobility indicators</u> are defined by some criteria relating to the mobility of mobile user. For example number of location updating or hand-over during a defined time
25 interval.

iii) <u>Deductive indicators</u> that arise as a result of a fraudulent behaviour: For example, use of conference calls, forwarded calls, etc.

As classifying indicators by way of use, the following
30 three categories can be identified:

- 11 -

i) <u>Primary indicators</u>, which in principle, can be employed in isolation to detect fraud. For example, the number of call-forwarding services invoked within a defined time interval.

ii) <u>Secondary indicators</u> from which, in principle, useful information can be gained if they are considered in isolation, but which should not be solely used to detect fraud. For example, information about cell sites or switch areas involved in a certain call handling, since Call-selling for certain destinations is concentrated in areas where the buyers live.

iii) <u>Tertiary indicators</u> from which no useful information can be gained if they are considered in isolation, but which can, in principle, be used to provide essential information in connection with the detection of fraud. For example, the number of successful hand-over within a defined time interval. In this respect, a fraudulent call-selling service requires a stable position so that a low mobility, accompanied by other activities with corresponding indicators, might identify possible fraudulent activities. Obviously, many mobile users may have this low mobility behaviour without performing any fraud so further detection of other activities is essential before being able to determine fraud.

Such an FDS is supposed to post-process these indicators to determine whether a fraudulent activity is occurring or, at least, suspicious of occurring.

These two main, separate, and not connected aspects hereinabove commented on, that is the actions performed on authentication failure and the needs for fraud detection,

- 12 -

are both background of the present invention as further justified in this description.

The Authentication procedure has been commented on for both 2G and 3G mobile networks. A new procedure, 5 "Authentication Failure Report", has been introduced for 3G mobile systems like UMTS, however, no corresponding procedure exists for some 2G system like GSM.

Nevertheless, specific vendor additions are provided to enhance and complete the current standards for 2G mobile 10 systems. For instance when an authentication failure is detected in an Ericsson provided MSC/VLR, said MSC/VLR logs all the relevant failure data, and activates an alarm. Said logging of authentication failure includes data such as date, time, IMSI, Mobile Subscriber ISDN number 15 (hereinafter referred to as MSISDN, wherein ISDN stands for Integrated Services Digital Network), Cell Global Identifier (hereinafter CGI), and whether the MAP message "Authentication Reject" was sent or not.

These vendor solutions imply that in a multi-vendor 20 and multi-operator environment it is not now possible to gather all the fraud related information regarding authentication failures for a single subscriber. Such an information would be stored in MSC/VLR from certain vendors whereas others will collect other authentication failure 25 data along the different serving networks. Under these assumptions, such a solution cannot be taken as a basis for introducing a standard fraud detection system given that an MSC/VLR vendor identifier should always be used as initial fraud criterion to analyse. Then, depending on the specific 30 MSC/VLR vendor, other available authentication failure data could be used for post-processing at the FDS.

- 13 -

Regarding fraud detection, other solutions exist in 2G mobile systems and have been adopted by different suppliers to some extent. One of the most common architecture to support fraud detection in mobile networks is illustrated in Fig.-3- where the FDS (N-1301) gathers the indicators required to perform the fraud analysis from the Call Data Records (hereinafter referred to as CDR) generated in the MSC/VLR (N-2122) or the SGSN (N-2112). Said CDRs are submitted through the Billing Gateway (N-2301) (hereinafter referred to as BGW), or any other Billing Mediation Device. As a consequence, the information received by the FDS is just related with the establishment of a call, whereas any other fraud related information, not call related, does not reach the FDS. This information is not received by the FDS by current means since it is not related with a call already established, and therefore there cannot be any CDR associated. For instance, fraud related information derived from an authentication failure does not imply any CDR to be received at the FDS under this solution. The case of call selling already commented on would have likely originated a CDR submitted in the past, whereas subsequent attempts to initiate such a call selling would get unsuccessful authentication results. In this respect, the fraud prevention is achieved, however, anyone skilled in the art can easily understand that fraud detection would be even worthwhile in order to know when new attempts to commit fraud are initiated.

On the other hand, and unlike 2G systems like GSM, there is an Authentication Failure Report procedure for IS-41 (TIA/EIA standards). Under said procedure, the report message is used by the Authentication Centre in IS-41 (hereinafter referred to as AC, unlike the one in GSM) in

- 14 -

order to decide whether the access for that subscriber will be denied, or a different action related with the standard security procedure is required. Nevertheless, no specific activity related with fraud detection is considered.

5   The Authentication procedure in IS-41 is not always performed in the same way. On the one hand, the VLR might have a Shared Secret Data (hereinafter referred to as SSD) that the AC had previously sent, so that the authentication data to be used in the authentication procedure are

10   obtained from said SSD. On the other hand, the VLR might receive the authentication data directly from the AC, in a similar way as is done for GSM, in order to use them in the authentication procedure. Whatever the case, when an authentication failure occurs (the response sent by the

15   user does not match the expected response hold by the VLR) the VLR does not make any decision but sends said authentication failure report to the AC. The AC then decides whether the access is denied or a new authentication must be performed. For the latter, the AC

20   also decides if new SSD is sent to the VLR, for said VLR to generate new authentication data, or if new authentication data are directly generated by the AC and sent to the VLR to be directly used in the new authentication procedure. What this procedure achieves is a centralised decision

25   mechanism to control the network.

At present, there is a new procedure introduced for UMTS, the "Authentication Failure Report" procedure already commented on above, which is merely intended to allow a centralised storage in the Home Environment (HE) for

30   authentication failure data. With such a mechanism the HE

- 15 -

can just control whether home subscribers are suffering or producing authentication failures.

However, the presently specified Authentication Failure Report procedure does not offer valuable
5   information yet from a fraud detection perspective to take further actions. In this respect, Fig.-4- shows the existing operation Authentication_Failure_Report as specified in 3G TS 29.002 for the Mobile Application Part protocol, in terms of Operation and Parameters.

10   Still another drawback, from the current solutions fraud detection related, is that the CDR only exist when there is a call already established, whereas nothing can be detected with this solution as the fraudulent user equipment is trying to gain access to the network.

15   **Summary of the Invention**

The object of the present invention is a method for providing relevant information for fraud detection which overcomes the above mentioned drawbacks.

In accordance with the present invention, data related
20   with unsuccessful authentication procedures, such us access type, authentication reattempt and server address, could be used for fraud detection.

The method gets advantage from the new introduced mechanism to report authentication failures in order to
25   provide more valuable information from a fraud detection perspective towards the Home Environment, including the steps of:

a) obtaining secondary fraud indicators from failures in user authentication procedures due to unsuccessful

- 16 -

network   authentications   or   unsuccessful   user
authentications

b) including said secondary fraud indicators as new
parameters of specific types in fields of the
5   Authentication Failure Report message (hereinafter referred
to as MAP AFR_req) sent from the Serving Environment (3G
MSC/VLR, 3G SGSN) back to the Home Environment (HE HLR) in
said authentication procedures

c) storing said messages in the Home Location Register
10   (HLR) for further processing.

Another object of the method of the present invention
is the forwarding of these fraud-related data collected in
the Home Environment towards an appropriate operator
specific device for Fraud Detection for processing in
15   conjunction with primary fraud indicators for fraud
detection purposes.

Brief Description of the Drawings

For the sake of clarity and a better understanding of
the scope and objects of the present invention, this
20   detailed description should be taken in conjunction with
the accompanying drawings, in which:

Fig.-1- is a block diagram representing a mobile
telecommunication system from a subscriber and network
authentication perspective. This system is structured
25   attending to different criteria:

- the Home Environment where the subscription resides
  versus the Serving Network where the subscriber is
  roaming;

- the Core Network versus the Access Network and the User
30   Equipment;

- 17 -

- the Circuit Switching services versus the Packet Switched
  services and corresponding network support.

Fig.-2- is a flow chart schematically representing the
authentication procedure as currently specified for 3G
5   mobile systems like UMTS networks.

Fig.-3- is another block diagram representing a
currently existing fraud detection system for call related
fraudulent activities

Fig.-4- shows the prior art MAP operation
10   Authentication_Failure_Report, as described by 3G TS 29.002
recommendations for UMTS, in terms of Operation and
Parameters.

Fig.-5- is the block diagram representing the
architecture required for a complete fraud detection system
15   accordingly with the present invention.

Fig.-6- is a flow chart schematically representing the
authentication procedure for 3G mobile systems like UMTS
networks in accordance with the present invention.

Fig.-7- presents the new MAP operation
20   Authentication_Failure_Report in terms of Operation and
Parameters in accordance with a preferred embodiment of the
present invention.

Fig.-8- is another flow chart schematically
representing the sending of the MAP operation
25   Authentication_Failure_Report with new proposed data, in
accordance to the present invention, storage of said data
in the HLR and further transmission of such data towards
the FDS for fraud analysis.

- 18 -

Detailed Description of Preferred Embodiments

There is very valuable information for fraud detection behind an authentication failure as explained hereinabove. The data related with authentication failure can never be used as primary indicator to detect fraud, since authentication is itself a method for fraud prevention, but said data can be used as secondary indicators so that further actions can be taken. However, the data sent in the UMTS Authentication Failure Report message are quite poor, from a fraud-detection point of view. Just the IMSI and the kind of failure are reported within such a MAP operation, as primary shown in Fig.-2- (S-240, S-270) and further stated in Fig.-4-.

On the other hand, there is quite valuable and significant information for fraud detection in the MSC/VLR, which is related or can be derived from an authentication failure. These significant data for fraud are considered as secondary indicators for fraud, and are part of fraud criteria in a Fraud Detection System.

In accordance with the present invention, other data already known by the MSC/VLR, when the authentication procedure shown in Fig.-2- takes place, should also be provided to the HE HLR within the MAP message Authentication Failure Report request (MAP AFR_req) (S-280, S-290)as shown in Fig.-6- and Fig.-7-. Some of said known data, relevant for fraud detection, are the following:

• Access type. In order to distinguish if the authentication procedure was initiated due to a call, an emergency call, a location updating, a supplementary service procedure or a short message transfer.

- 19 -

- Authentication reattempt. This indicates whether the failure was produced in a normal authentication attempt or it was due to an authentication reattempt. The latter indicates that there was a previous unsuccessful
5   authentication.

- Server address. It indicates the address of the network element, either SN MSC/VLR or SN SGSN, where the authentication procedure took place. This data shall be included in order to have a reference to the physical
10   location where the authentication failure had been produced.

Each of the three new parameters has its own advantage in accordance with the present invention.

The access type parameter can be used to evaluate the
15   seriousness of the failure since it can be considered more serious a failure produced in a location updating than in a call set up, and the latter more serious than the one produced in a short message transfer. These considerations are based on some facts; for example, a successful location
20   updating has to be performed previous to an unsuccessful call.

The authentication reattempt parameter is sent in order to know if the failure was produced on a first authentication procedure or during a reattempt. An
25   authentication reattempt is performed in current networks since the failure could have been provoked by a Temporary Mobile Station Identity (hereinafter TMSI) mismatch, or by erroneous Authentication Vectors received from the previous MSC/VLR or SGSN server (the reattempt is performed after
30   requesting new Authentication Vectors to the HLR). When the

- 20 -

authentication reattempt is performed, the corresponding procedure is carried out with the correct IMSI (User Identity Request performed) and with correct Authentication Vectors (Send Authentication Info performed), thus an error
5   in this case is of higher importance.

The interest of the server address from a fraud-detection point of view resides in the fact that some fraudulent activities like call selling in current mobile networks are associated with concrete geographical
10 location.

These and other data not explained yet are identified as being of interest for a Fraud Detection System (FDS) as secondary indicators, and part of the fraud criteria analysis in said FDS. When new fraudulent activities are
15 identified, new data will be found to be interesting as fraud indicators, and still part of the present invention. The scope of the present invention is not intended to be restricted to only these three identified and explained new data, to be included within the existing MAP AFR_req
20 message, as anyone skilled in the art may easily understand. For example, and as an additional embodiment of the present invention, provided that the severity of fraud requires more accurate information about the geographical position where the fraud is committed, the user equipment
25 position got by means of GPS facilities could also be sent in the MAP AFR_req message. As anyone skilled in the art may easily understand, known data at the MSC/VLR or SGSN, which are significant for fraud detection, can be included in the MAP AFR_req message. In this way, these data can be
30 eventually submitted to the HE HLR and from there forwarded to an appropriate Fraud Detection System like the FDS.

- 21 -

In accordance with Fig.-7-, the proposal of a preferred embodiment of the present invention is that these data, namely the Access Type, the Authentication Reattempt, and the Server Address should be including as new specific
5   parameters within the MAP AFR_req message. Moreover, still under a preferred embodiment of the invention, the Server Address should be better expressed in terms of different parameters such as MSC/VLR_address and SGSN_address in order to identify on what service, Circuit or Packet, the
10 authentication has failed.

In accordance with the message and parameters format specified by 3G TS 29.002, the following new parameters could be included for the existing MAP message "authenticationFailureReport_req" in said specifications,
15 3G TS 29.002, as Fig.-7- states.

   • "authenticationReattempt" of type "BOOLEAN"

   • "accessType" of a new type "AccessType"

   • "vlr-Number" of type "[0] ISDN-AddressString"

   • "sgsn-Number" of type "[1] ISDN-AddressString"

20   Furthermore, the new type above introduced "AccessType" could also be declared following the ASN.1 notation as "ENUMERATED" with the following assignations: Call (0), emergencyCall (1), locationUpdating (2), supplementaryServices (3), shortMessage (4). As anyone
25 skilled in the art can easily understand re-ordering the previous assignations will not substantially affect the object of the present invention under this preferred embodiment.

- 22 -

Moreover, the inclusion of these new data above mentioned in the MAP AFR_req operation, in accordance with the preferred embodiment of the invention as shown in Fig.- 7-, should be understood in an illustrative and non-
5   restrictive manner. In this respect, a secondary embodiment of the present invention suggests the inclusion of these new data above within the Extension Container field.

The MAP AFR_req message definition allows the introduction of new parameters in an extension container.
10   All the data proposed in the present invention, as fraud indicators, could be included in the mentioned extension container.

Said extension container can be regarded as the means to introduce proprietary information in a standard message
15   and thus, provided that the fraud indicators are included there, the result will be a proprietary solution to some extent.

As already stated above, one of the main objects of the present invention is that any operator can gather all
20   the fraud information related with authentication faults from its own subscribers. With a proprietary solution this would not be achieved since the reception of that information would directly depend on the VLR/SGSN supplier and therefore it would indirectly depend on the serving
25   operator (roaming situation for the subscriber). As a consequence, an operator could not gather all the fraud information regarding authentication fraud from its own subscribers. Nevertheless, though less efficient than the preferred embodiment, this second embodiment of the present
30   invention also proposes reasonable means to provide an FDS with the required secondary indicators for fraud detection.

- 23 -

A further process step of the present invention is the reception of these new fraud related data, included in the MAP AFR_req operation, in the HE as Fig.-8- illustrates.

At reception of the MAP AFR_req message (S-700) the
5 HLR will store the received data together with the time and date of the report (B-500).

When the number of failures reaches a given threshold value (B-510) for a certain subscriber an alarm shall be issued at the HLR (B-520). The value for such a threshold
10 that triggers the alarm shall be configurable.

Next, an "Authentication Failure Alarm" (S-710) will be addressed to the Operation and Maintenance Gateway (hereinafter referred to as OMG) in the operator network. Then, through that Gateway said Authentication Failure
15 Alarm (S-720) will reach the FDS.

On reception of such an alarm, the FDS would use the commands through the Operation and Maintenance Gateway (S-730) to request the stored logging of authentication failures (S-740) in HLR. Thus, the HLR logging regarding
20 authentication failure report log shall be addressed as well to the Operation and Maintenance Gateway (S-750), so that they can be eventually forwarded to the FDS (S-760). Further, the FDS can analyse the received secondary indicators for fraud in conjunction with applicable fraud
25 criteria (B-530). Moreover, these secondary indicators will be used in the FDS in conjunction with some primary indicators, as the number of call forwarding within a defined time interval, to detect fraud situations such as SIM cloning.

30

- 24 -

CLAIMS

1.- A method for fraud detection in mobile telecommunications systems comprising the steps of:

5   a) obtaining secondary fraud indicators from failures in user authentication procedures due to unsuccessful network authentications or unsuccessful user authentications;

b) including said secondary fraud indicators in the
10   authentication failure report message (MAP AFR_req) sent from the Serving Environment (3G MSC/VLR, 3G SGSN) back to the Home Environment (HE HLR) in said authentication procedures, as new parameters of specific types for each of said indicators; and

15   c) storing said messages in the Home Location Register (HLR) for further processing.

2.- A method according to claim 1, further comprising the step of forwarding an alarm message to a Fraud Detection System (FDS) entity through the Operation and
20   Maintenance Gateway (OMG) when the number of authentication failures of an user exceeds a predetermined value.

3.- A method according to claim 1 or 2, further comprising the step of processing authentication failure report messages (AFR_req) in the fraud detection System
25   (FDS) entity in conjunction with primary fraud indicators, for fraud detection purposes, having obtained said messages from the Home Location Register (HLR).

4.- A method according to any of the preceding claims, characterized in that said secondary fraud indicators
30   includes the access type of the communication in which the authentication procedure failed.

5. A method according to claim 4, characterized in that said access type corresponds at least to a call, an

- 25 -

emergency call, a location updating, a supplementary service procedure or a short message transfer.

6.- A method according to any of the preceding claims, characterized in that said secondary fraud indicators includes a re-attempt indicator indicating whether the authentication failure was produced in a normal authentication attempt or in a authentication reattempt.

7.- A method according to any of the preceding claims characterized in that said secondary fraud indicators includes the Visitor Location Register (VLR) or the Serving GPRS Support Node (SGSN) address.

8.- A method according to any of the preceding claims characterized in that said secondary fraud indicators are included in extension container fields of said authentication failure report message (MAP AFR_req) instead of new parameters of specific types.
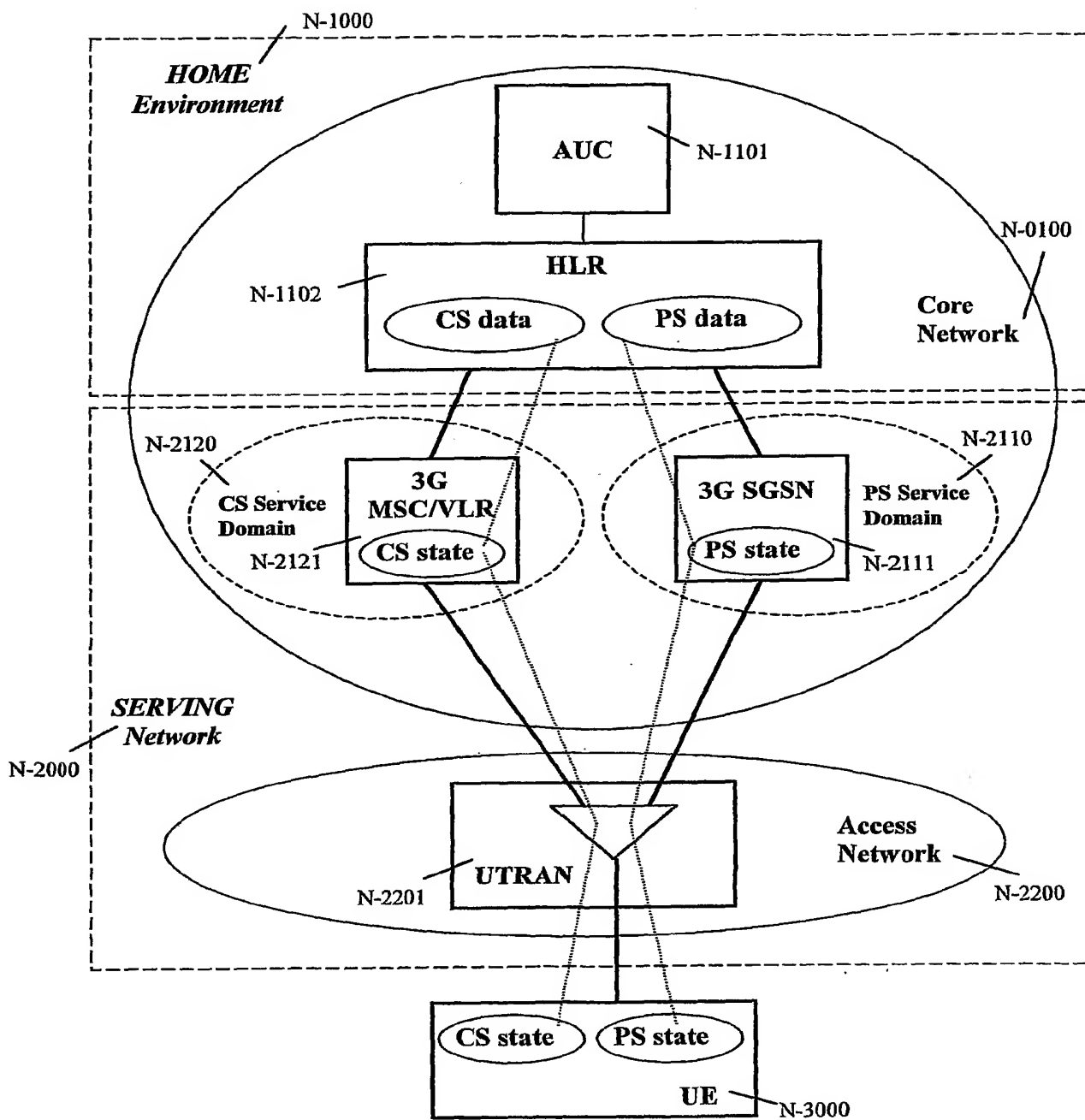
FIG.-1-
Prior Art

FIG.-2-
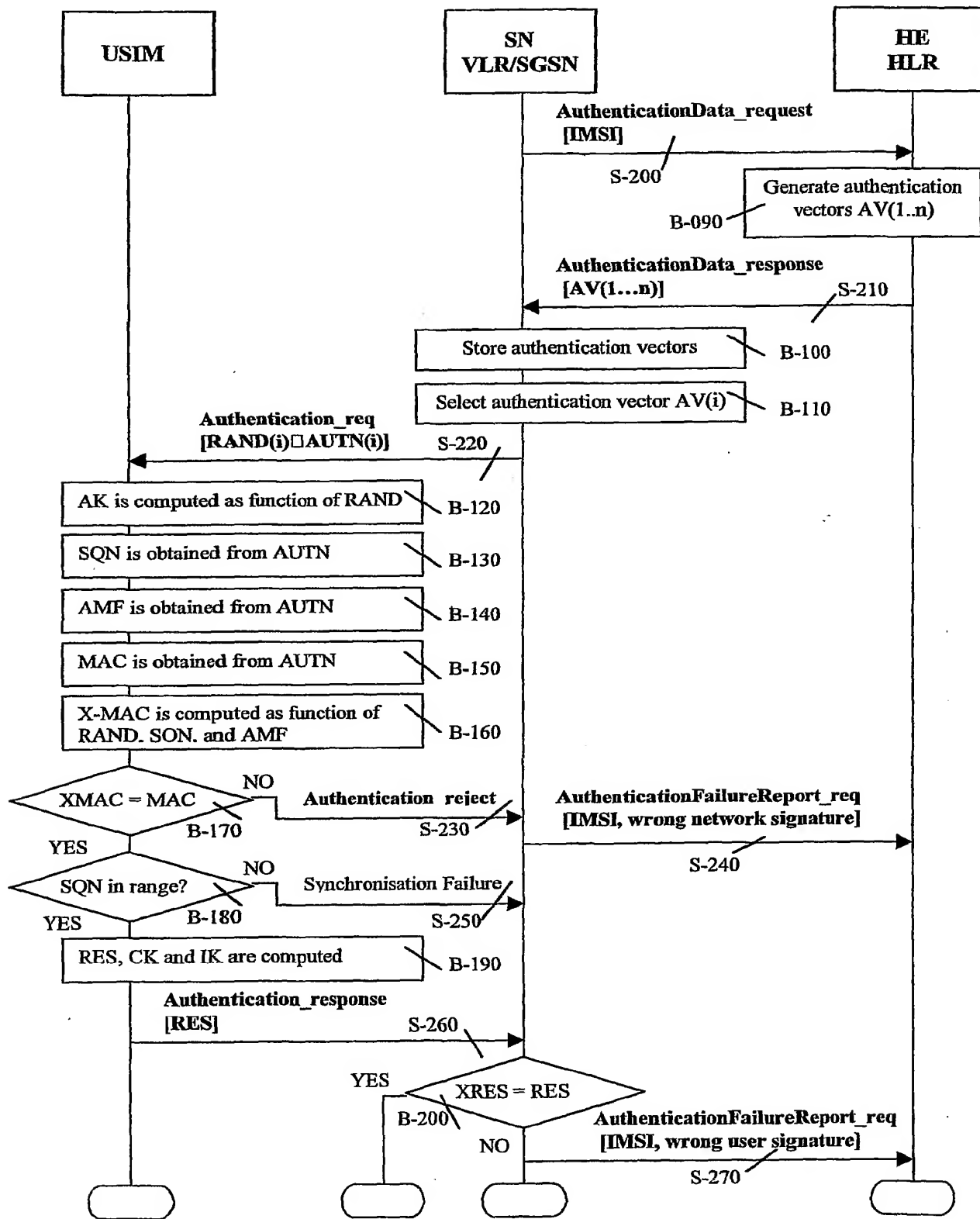Prior Art

N-1000

HOME
Environment

FDS — N-1301

N-2000

SERVING
Network

SGSN

N-2112

BGW

N-2301

MSC/VLR

Core
Network

N-0100

N-2122

Mediation
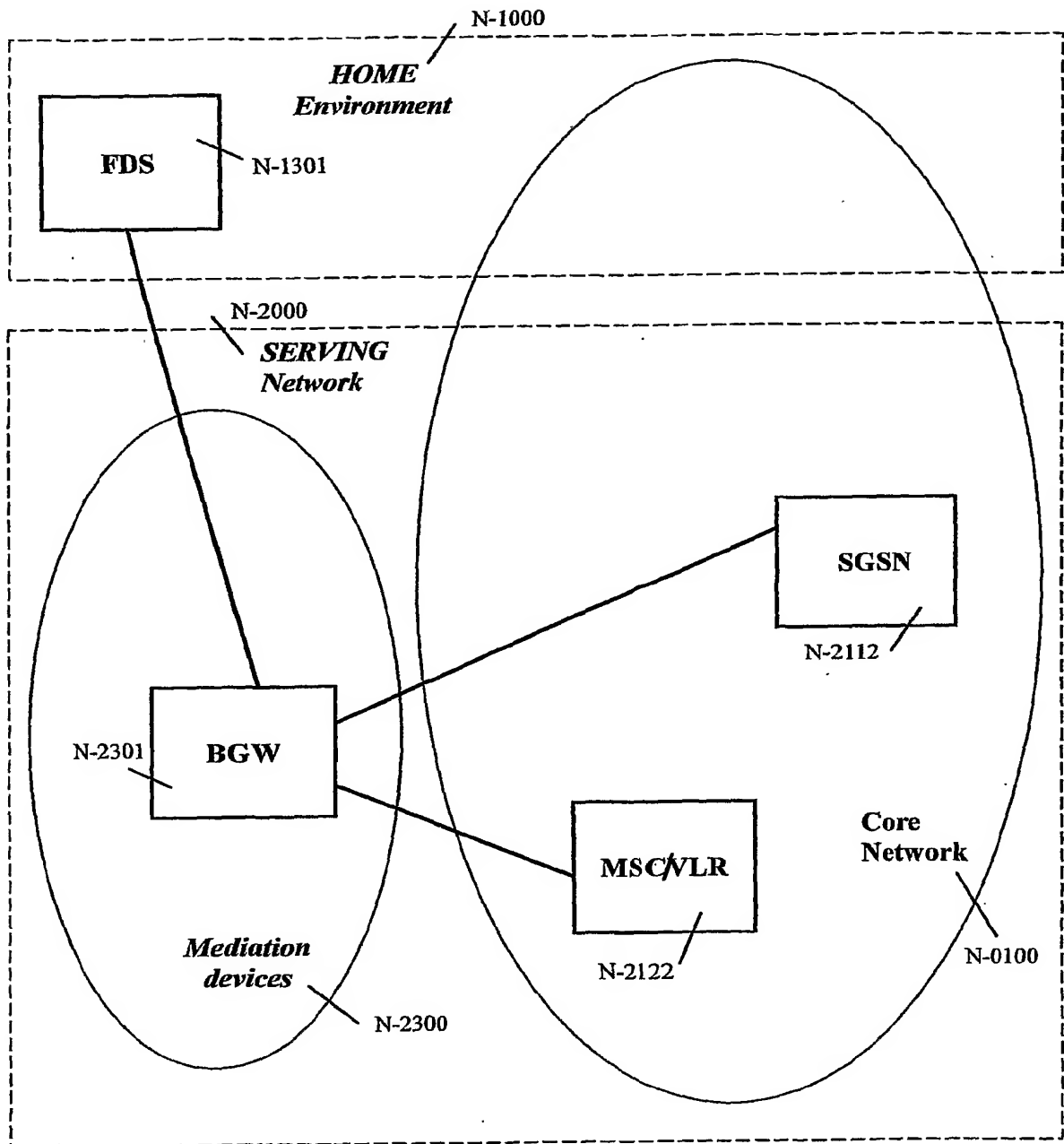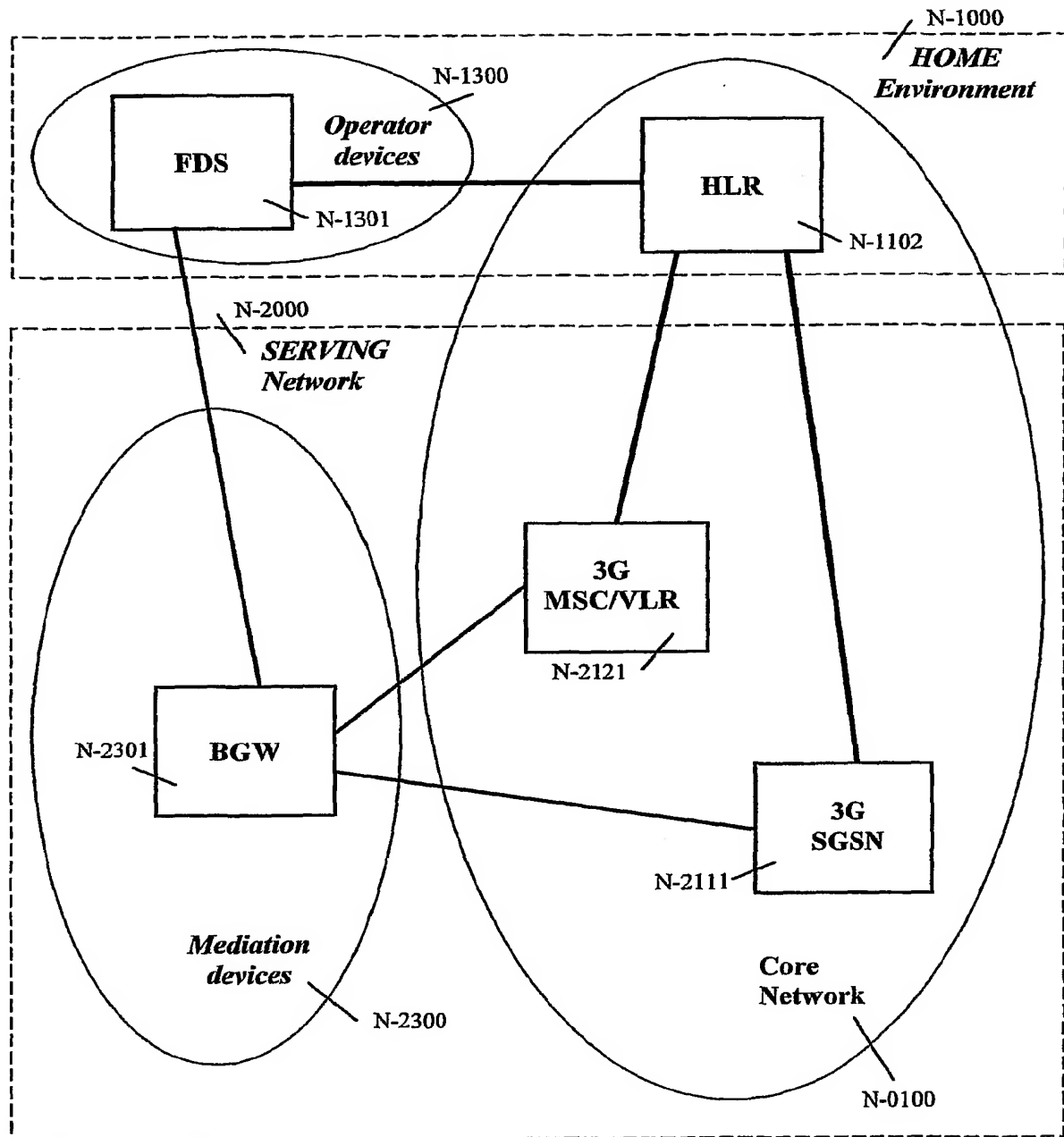devices

N-2300

FIG.-3-
Prior Art

```
AuthenticationFailureReport ::= OPERATION          --Timer m
       ARGUMENT
              authenticationFailureReportArg        AuthenticationFailureReportArg
       RESULT
              authenticationFailureReportRes        AuthenticationFailureReportRes
              -- optional
       ERRORS  {
              SystemFailure, {
              UnexpectedDataValue,
              UnknownSubscriber  }
```

```
AuthenticationFailureReportArg ::= SEQUENCE {
       imsi                    IMSI,
       failureCause            FailureCause,
       extensionContainer      ExtensionContainer          OPTIONAL,
       ... }
```

```
FailureCause ::= ENUMERATED {
       wrongUserResponse            (0)
       wrongNetworkSignature        (1) }
```

FIG.-4-
Prior Art

FIG.-5-

FIG. -6 -
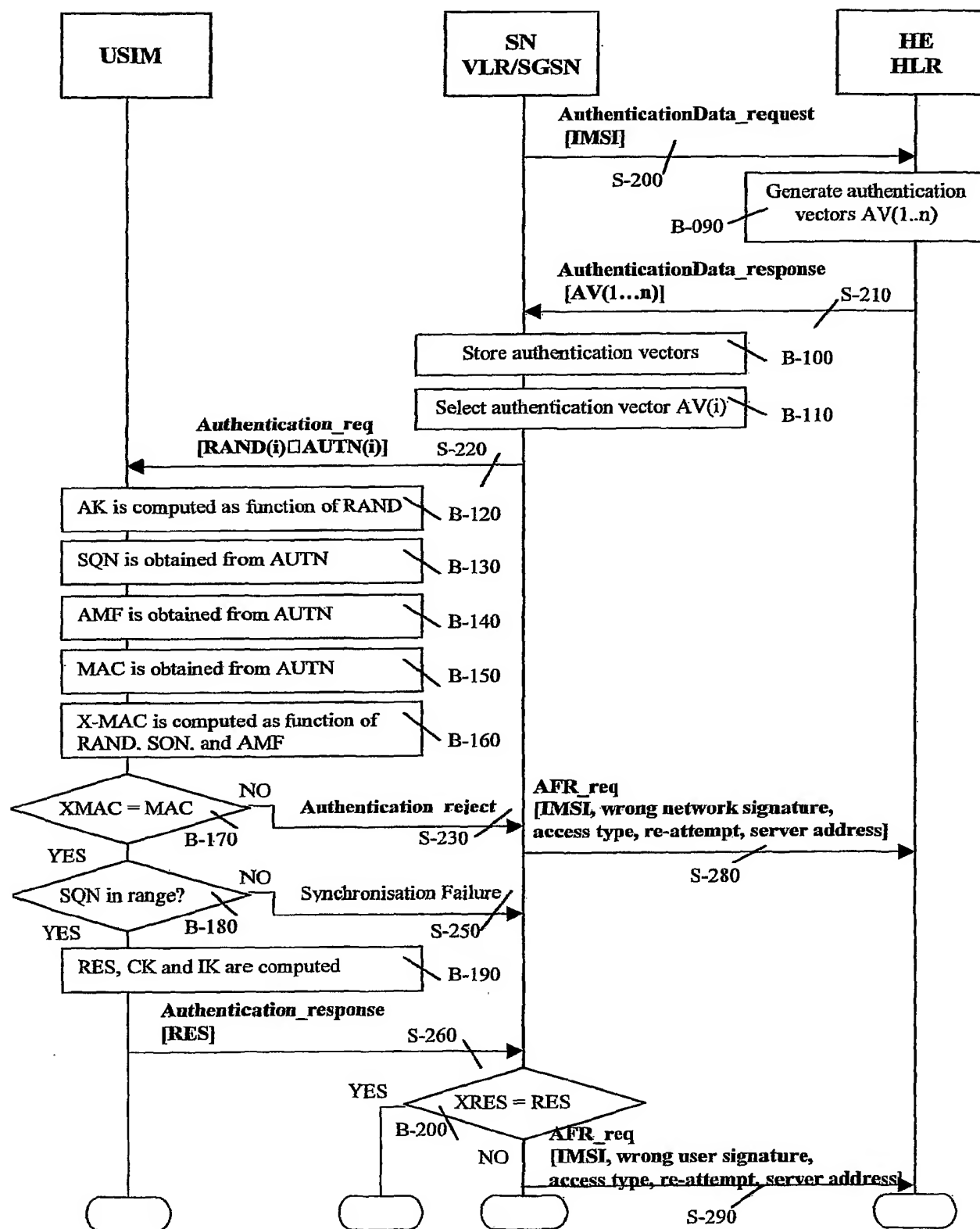
```
AuthenticationFailureReport ::= OPERATION          --Timer m
        ARGUMENT
                authenticationFailureReportArg     AuthenticationFailureReportArg
        RESULT                          .
                authenticationFailureReportRes     AuthenticationFailureReportRes
                -- optional
        ERRORS {
                SystemFailure, {
                UnexpectedDataValue,
                UnknownSubscriber }
```

```
AuthenticationFailureReportArg ::= SEQUENCE {
        imsi                    IMSI,
        failureCause            FailureCause,
        accessType              AccessType,
        re-attempt              BOOLEAN,
        vlr-Number              [0]   ISDN-AddressString    OPTIONAL,
        sgsn-Number             [1]   ISDN-AddressString    OPTIONAL,
        extensionContainer      ExtensionContainer          OPTIONAL,
        ... }
```

```
AccessType ::= ENUMERATED {
        call                    (0)
        emergencyCall       .   (1)
        locationUpdating        (2)
        supplementaryService    (3)
        shortMessage            (4) }
```
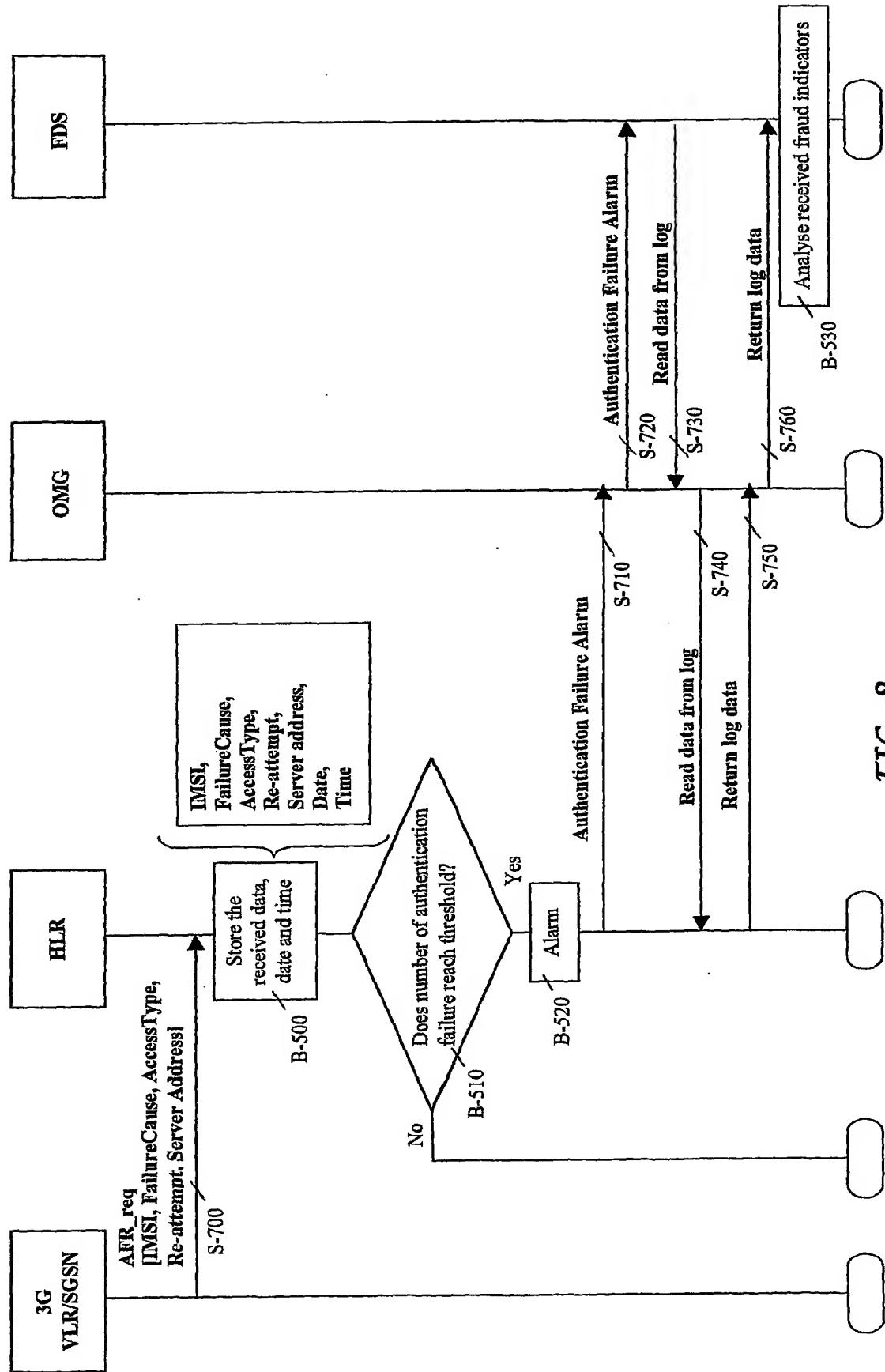
FIG.-7-

FIG. -8-

INTERNATIONAL SEARCH REPORT

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7   H04Q7/38

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7   H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category°	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 6 038 555 A (BARSON PAUL COLIN ET AL) 14 March 2000 (2000-03-14) column 3, line 56 -column 4, line 13 column 10, line 18 - line 33 column 18, line 14 - line 36 column 26, line 6 - line 35 ---	1-8
A	US 5 991 617 A (POWELL MICHAEL B) 23 November 1999 (1999-11-23) column 1, line 38 - line 63 column 2, line 66 -column 3, line 10 column 3, line 48 - line 58 column 6, line 5 - line 16 ---	1-8
A	EP 0 544 095 A (MOTOROLA INC) 2 June 1993 (1993-06-02) column 2, line 3 - line 16 column 4, line 56 -column 5, line 33 ------	1-8

☐ Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
28 February 2002	08/03/2002

Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Authorized officer Dionisi, M

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
US 6038555	A	14-03-2000	GB	2321362 A	22-07-1998
			AU	5770998 A	07-08-1998
			CA	2249321 A1	23-07-1998
			EP	0886831 A1	30-12-1998
			WO	9832085 A1	23-07-1998
US 5991617	A	23-11-1999	NONE		
EP 0544095	A	02-06-1993	DE	69230716 D1	06-04-2000
			DE	69230716 T2	28-12-2000
			EP	0544095 A1	02-06-1993
			US	5708969 A	13-01-1998